Supreme Court, U.S.
FILED
JAN 14 2009
OFFICE OF THE CLERK

17 (52)

No. 08-765

# In the Supreme Court of the United States

COMMONWEALTH OF VIRGINIA,
*Petitioner,*
v.
JEREMY JAYNES,
*Respondent.*

ON PETITION FOR A WRIT OF CERTIORARI TO THE SUPREME COURT OF VIRGINIA

## BRIEF FOR THE UNITED STATES INTERNET SERVICE PROVIDER ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

JENNIFER C. ARCHIE
*Counsel of Record*
ALEXANDER MALTAS
CATHERINE A. BELLAH
LATHAM & WATKINS LLP
555 11TH STREET, NW
SUITE 1000
WASHINGTON, DC 20004
(202) 637-2200

## QUESTION PRESENTED

Whether the Virginia Supreme Court erred by invalidating an important criminal statute under the First Amendment overbreadth doctrine absent evidence that any potential unconstitutional applications of the statute are real and substantial in comparison to the statute's legitimate sweep.

## TABLE OF CONTENTS

Page

QUESTION PRESENTED ..... i

TABLE OF CONTENTS ..... ii

TABLE OF AUTHORITIES ..... iv

INTEREST OF *AMICUS CURIAE* ..... 1

SUMMARY OF ARGUMENT ..... 2

ARGUMENT ..... 4

I. SPAM IMPOSES MASSIVE COSTS AND IS A LEGITIMATE TARGET OF CRIMINAL PROSECUTION ..... 4

A. Spam Causes Significant Injury to the Private Networks of Internet Service Providers ..... 4

B. ISPs Make Every Effort To Keep Spammers Off Of Their Private Networks ..... 8

C Federal And State Laws Properly Create Civil And Criminal Penalties For Spamming ..... 10

II. LOWER COURTS ARE CONFUSED OVER HOW TO APPLY THE OVERBREADTH DOCTRINE ..... 10

A. The Overbreadth Doctrine Is "Strong Medicine" And Is Necessarily Narrow And Limited ..... 12

## TABLE OF CONTENTS—Continued

Page

B. The Virginia Supreme Relied On Hypothetical Scenarios That Have No Basis in Actual Fact ..... 13

C. Lower Courts Are In Disarray Over How To Apply The Overbreadth Doctrine ..... 17

CONCLUSION ..... 19

# TABLE OF AUTHORITIES

Page(s)

## CASES

*Broadrick v. Oklahoma*,
413 U.S. 601 (1973) ..... 12

*CompuServe, Inc. v. Cyber Promotions, Inc.*,
962 F. Supp. 1015 (S.D. Ohio 1997) ..... 6

*EarthLink, Inc. v. Carmack*,
No. 1:02-CV-3041-TWT, 2003 U.S. Dist. LEXIS 9963 (N.D. Ga. May 7, 2003) ..... 6

*Hill v. Colorado*,
530 U.S. 703 (2000) ..... 12, 13

*McIntyre v. Ohio Elections Commission*,
514 U.S. 334 (1995) ..... 14

*Members of City Council of Los Angeles v. Taxpayers for Vincent*,
466 U.S. 789 (1984) ..... 13

*Milavetz, Gallop & Milavetz, P.A. v. United States*,
541 F.3d 785 (8th Cir. 2008) ..... 18

*New York State Club Association v. City of New York*,
487 U.S. 1 (1988) ..... 12, 17

*State v. Casey*,
876 P.2d 138 (Idaho 1994) ..... 18

## TABLE OF AUTHORITIES—Continued

Page(s)

*State v. Heckel*,
24 P.3d 404 (Wash.), *cert. denied*, 534 U.S. 997 (2001) ..... 9

*United States v. Williams*,
128 S. Ct. 1830 (2008) ..... 13, 16, 17

*Virginia v. Hicks*,
539 U.S. 113 (2003) ..... 12

### STATUTES

15 U.S.C. § 7701 et seq ..... 6

15 U.S.C. § 7707(b)(2) ..... 7

Va. Code Ann. § 18.2-152.3:1 ..... 2, 10, 13, 16

### OTHER AUTHORITY

Federal Trade Commission, National Do Not Email Registry: A Report to Congress (June 2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf ..... 5

**TABLE OF AUTHORITIES—Continued**

**Page(s)**

International Telecommunications Union, ITU Study on the Financial Aspects of Network Security: Malware and Spam 22, 27 (July 2008), *available at* http://www.itu.int/ITU-D/cyb/cybersecurity/ docs/itu-study-financial-aspects-of-malware-and-spam.pdf.....8

Messaging Anti-Abuse Working Group, Email Metrics Report: The Network Operators' Perspective, Report #1 – 4th Quarter 2005 Report 2 (Mar. 2006), *available at* http://www.maawg.org/about/AAWG_2005-4Q-Metrics_Report.pdf .....7

Messaging Anti-Abuse Working Group, Email Metrics Report: The Network Operators' Perspective, Report #9 – Second Quarter 2008 2 (Oct. 2008), *available at* http://www.maawg.org/about/MAAWG_2008-Q2_Metrics_Report9.pdf .....7

S. Rep. No. 108-102 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348.....5, 7

## INTEREST OF *AMICUS CURIAE*

The United States Internet Service Provider Association ("US ISPA") is a trade association that serves as the Internet Service Provider ("ISP") community's representative in common policy and legal matters. US ISPA represents many of the country's largest ISPs.

US ISPA and its members have a vital interest in the proper resolution of this case. US ISPA's members receive billions of unsolicited bulk electronic messages (sometimes referred to as "spam") through their servers every day, and have invested significant resources to attempt to filter and block spam on behalf of their subscribers. Sending spam with deceptive transmission information designed to bypass ISPs' filters, including the criminal behavior at issue in this case, imposes direct and substantial injuries on US ISPA members. In addition, US ISPA and its members have actively worked with federal and state legislatures and law enforcement officers to protect the operation of the Internet while promoting interstate commerce. As a result of its members' ongoing efforts to combat spam, US ISPA has a unique understanding of the practical and legal considerations relevant to the interpretation of laws combating spam.[1]

---

[1] Pursuant to Rule 37.6, US ISPA states that no counsel for any party authored this brief in whole or in part, and no person or entity other than the US ISPA and its members made any monetary contribution to the preparation or submission of this brief. Both parties received timely notice of US ISPA's intent to file this brief, and both parties granted consent.

## SUMMARY OF ARGUMENT

Respondent Jeremy Jaynes, one of the most notorious spammers, was convicted of sending tens of thousands of spam messages through privately-owned network facilities in Virginia. His spam e-mails peddled such products as a "penny stock picker," a FedEx refunds claim product, and an Internet history eraser product. During a search of his home, police found compact discs containing over 100 million e-mail addresses of AOL subscribers—a purchased copy of a stolen database of every AOL subscriber. He was convicted under a provision of the Virginia Computer Crimes Act ("VCCA") that makes it a crime to "use[] a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers." Va. Code Ann. § 18.2-152.3:1.

Respondent concedes that this statute is constitutional as applied to him, and that his unlawful conduct is a legitimate target of criminal prosecution. He argued below that his conviction should be reversed because the statute may be unconstitutional as applied to *others*—*i.e.*, that it is unconstitutionally overbroad. The Virginia Supreme Court agreed, holding that the language of the statute might reach hypothetical speakers who wish to engage in anonymous political or religious speech by sending bulk unsolicited e-mails, and concluding on that ground that the statute is unconstitutional.

The Virginia Supreme Court's ruling distorts the overbreadth doctrine, and reflects a more general

confusion among lower courts over how to apply the doctrine. The Virginia Supreme Court cited no evidence in the record that any anonymous political or religious speakers actually exist who attempt to broadcast their messages by sending tens of thousands of unsolicited bulk messages using forged routing or transmission information. As US ISPA explains below, the court could not cite any such evidence because its hypothetical scenarios have no grounding in reality. The Thomas Paines or Publiuses of the world have many ways to speak anonymously on the Internet and through e-mail, and even a cursory search of the Internet shows that such speakers are thriving online. In the real world, as US ISPA and its members are acutely aware, spammers—who send billions of unsolicited messages each day using forged header information to evade e-mail filters—are not spreading the messages of political dissidents or oppressed religious sects. Rather, they are abusing the Internet to peddle commercial products and defraud consumers, shifting the substantial costs and burdens associated with processing and transmitting such spam onto private network owners. The potentially unconstitutional applications of this statute are thus purely hypothetical, with no basis in actual fact, and cannot justify a holding that the statute is unenforceable in all contexts.

Had respondent been required to make a factual showing of substantial overbreadth (rather than merely positing fanciful hypotheticals), the Virginia Supreme Court would have seen that there is no basis to conclude that the VCCA has any meaningful impact on protected expression. Had the court compared the statute's legitimate sweep to any such tiny (or

nonexistent) restriction on protected speech, it would have affirmed respondent's conviction. Unfortunately, the court abdicated that responsibility, and invalidated an important statute based on far-fetched hypotheticals untethered to any factual record or legislative findings, or even any real world scenarios.

As US ISPA demonstrates below, spam is a serious problem that is properly and narrowly targeted by the VCCA. This Court should grant certiorari to reverse the erroneous invalidation of the Commonwealth's statute and provide the lower courts needed guidance on the proper application of the overbreadth doctrine.

## ARGUMENT

### I. SPAM IMPOSES MASSIVE COSTS AND IS A LEGITIMATE TARGET OF CRIMINAL PROSECUTION

#### A. Spam Causes Significant Injury to the Private Networks of Internet Service Providers

Nearly everyone with an e-mail account sends, receives, and accesses e-mail through a third-party service provider, whether that provider is their employer, or, more commonly, a private electronic mail service provider ("ISP").[2] Sending an e-mail therefore involves more parties than merely the sender and receiver. Such e-mails must be filtered, processed, routed, and stored by the recipient's ISP on the ISP's servers and internal network. ISPs have made substantial investments in their infrastructure to

---

[2] Electronic mail service is one service typically provided by an Internet Service Provider. For convenience, we refer to electronic mail service providers by the more commonly-used acronym "ISP."

handle the billions of e-mails sent, received, and stored each day.

Because sending e-mail to an ISP's subscriber imposes costs and burdens on the ISP's facilities and resources, every ISP of which US ISPA and its members are aware prohibits the sending of unsolicited bulk e-mail through their facilities. Despite those clear prohibitions, spammers nonetheless send billions of such messages each day through ISPs' private networks. The record in this case shows that AOL's mail servers alone received over 1 billion e-mails every day; that at least 70 to 80 percent of those e-mails were spam; and that AOL received 7 to 10 million complaints per day from customers about spam. *See* Pet. App. 102. Congress found that, in 2003, more than 2 trillion spam e-mails were estimated to be sent over the Internet, two-thirds of which would contain fraudulent content.[3] The Federal Trade Commission has stated that spam is being used increasingly as a vehicle for "phishing," (which refers to sending a fraudulent e-mail masquerading as from a trustworthy source in order to acquire sensitive information such as bank account numbers or social security numbers).[4] Spam is also used increasingly for inducing people to download harmful viruses or other malicious software.[5]

---

[3] S. Rep. No. 108-102, at 3, 2 (2003), *as reprinted in* 2004 U.S.C.C.A.N. 2348, 2349.

[4] Federal Trade Commission, National Do Not Email Registry: A Report to Congress 16 & n.76 (June 2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf ("FTC Report").

[5] FTC Report at 1, 10, 24.

ISPs' mail servers and spam filters have finite processing speed and memory storage capacity, and the massive volume of spam e-mails destabilized their networks by reducing system reliability and efficiency. One court aptly summarized this problem: "High volumes of junk e-mail devour computer processing and storage capacity, slow down data transfer between computers over the Internet by congesting the electronic paths through with the messages travel, and cause recipients to spend time and money wading through messages that they do not want." *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1028 (S.D. Ohio 1997). The spam nuisance also damages the ISP's goodwill and the value of its reputation and brand. Spam costs ISPs billions of dollars a year due to the burdens spam imposes on their networks, the costs of filtering and preventing spam from reaching subscribers, and the lost goodwill and confidence due to consumers' frustrations.[6]

Indeed, Congress has recognized the severity of the problem and enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7701 et seq. ("CAN-SPAM Act"), to help address the spam problem. After years of hearings and extended debate concerning the spam problem, Congress made several findings: (1) spam imposes costs on individuals who must access, review, and discard unwanted spam; (2) spam decreases the convenience and utility of e-mail; (3) spam creates a risk that desired e-mails will be lost amid a torrent of

---

[6] In a recent case, a court found that one spammer alone inflicted millions of dollars in direct damages by flooding an ISP with spam. *See EarthLink, Inc. v. Carmack*, No. 1:02-CV-3041-TWT, 2003 U.S. Dist. LEXIS 9963, at *17 (N.D. Ga. May 7, 2003).

unwanted spam; and (4) spam imposes significant costs on ISPs, businesses, and schools, which must spend more money to acquire the infrastructure necessary to handle the increased e-mail traffic. S. Rep. No. 108-102, at 5-7, *as reprinted in* 2004 U.S.C.C.A.N. at 2352-53. Congress believed that "spam may soon undermine the usefulness and efficiency of e-mail as a communications tool." *Id.* at 6, *as reprinted in* 2004 U.S.C.C.A.N. at 2352. Congress in 2003 estimated that spam costs Internet subscribers $9.4 billion per year and would likely cost corporations over $113 billion by 2007. Employee productivity losses alone from sifting through and deleting spam accounted for nearly $4 billion in 2003. *Id.* at 6-7, *as reprinted in* 2004 U.S.C.C.A.N. at 2353. Congress recognized the need for a variety of laws to address this large problem, and specifically excepted from preemption state laws, like the VCCA, that seek to curb fraudulent and criminal spam. 15 U.S.C. § 7707(b)(2).

Since Congress made its fact findings in 2003, the volume of spam messages sent has not declined. A recent report found that approximately 85% of all attempted e-mails are "abusive" spam.[7] Another study found that worldwide spam levels averaged 84.6% of

---

[7] Messaging Anti-Abuse Working Group ("MAAWG"), Email Metrics Report: The Network Operators' Perspective, Report #9 – Second Quarter 2008 2 (Oct. 2008), *available at* http://www.maawg.org/about/MAAWG_2008-Q2_Metrics_Report9.pdf; MAAWG, Email Metrics Report: The Network Operators' Perspective, Report #1 – 4th Quarter 2005 Report 2 (Mar. 2006), *available at* http://www.maawg.org/about/MAAWG_2005-4Q-Metrics_Report.pdf.

the total number of e-mails for 2007.[8] Approximately 80% of that spam is distributed through networks of compromised personal computers under the control of cyber criminals, commonly known as botnets.[9] Additionally, the instances of web-based attacks by malicious software, of which spam is a leading source, continued to rise over the last several years.[10]

### B. ISPs Make Every Effort To Keep Spammers Off Of Their Private Networks

Network owners attempt to protect their private property from the abuse inflicted by spam by deploying technical filtering software to identify and block as much spam as possible from reaching the mailboxes of their subscribers. ISPs do not employ spam filters out of some abstract opposition to anonymous speech; they employ spam filters because their customers overwhelmingly demand it and because the physical limitations on the size of their networks require it. ISPs' anti-spam measures involve highly sophisticated technological filters that, among other things, identify computers that previously sent spam and then block messages sent by those computers from reaching

---

[8] *See* International Telecommunications Union, ITU Study on the Financial Aspects of Network Security: Malware and Spam 22, 27 (July 2008), *available at* http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf ("ITU Study").

[9] *Id.* Computer hackers create botnets by transmitting malicious codes (most often through spam) to thousands of personal computers. Once downloaded, the code infects the computer so that it acts essentially as a robot drone for the hacker controlling the botnet.

[10] ITU Study. at 20-22.

subscriber mailboxes. These anti-spam measures are expensive to develop and maintain, and require significant technical and personnel resources. AOL, for example, employs a staff of 30 people dedicated solely to its spam response team.

Spammers resort to elaborate methods to elude ISPs' spam filters and surreptitiously gain access to private networks that would otherwise bar them. One of the most common ways spammers seek to evade the filters is by forging their messages' routing or transmission information so that tens of thousands of messages sent from a single sender appear to originate from many sources. Spammers thus deliberately disguise the source of their spam by masking the computer from which the e-mail is sent in order to send billions of messages through ISPs who are making every effort to bar them by identifying and blocking their source.

Spammers who evade these anti-spam filters effectively shift the costs of distributing their messages onto ISPs. Instead of using alternative means of distributing their messages, for which they might otherwise pay postage, delivery fees, or advertising space, spammers force ISPs to shoulder the burden of transmission, processing, and storing those messages. *See State v. Heckel*, 24 P.3d 404, 410 (Wash.) ("This cost-shifting—from deceptive spammers to businesses and e-mail users—has been likened to sending junk mail with postage due ...."), *cert. denied*, 534 U.S. 997 (2001). The economic reality is that spam has grown exponentially because, from the spammer's perspective, it is virtually free to send. Every other method a marketer could use to sell his products, from

direct mail to television advertising to renting a billboard, costs money.

### C. Federal And State Laws Properly Create Civil And Criminal Penalties For Spamming

State and federal laws against spam are important to protect ISPs and their customers. Indeed, Congress and 43 states, including Virginia, have enacted anti-spam laws in order to impose civil and criminal deterrents to spamming. The types of anti-spam provisions exemplified by the statute at issue in this case are vital to protect the property and security of ISPs and their subscribers from spammers and from any malicious software or other harmful applications their spam may contain.

ISPs, legislators, and law enforcement have been working together to combat the spam problem. Technical filters alone are inadequate to prevent spam as evidenced by the millions of spam complaints that AOL alone receives daily. Legislation such as the VCCA is also a necessary tool in the battle. The VCCA provides valuable deterrence in the form of criminal sanctions for those who attempt to evade private network owners' technical defenses in order to send spam. This Court should be reluctant to condone a ruling that invalidated a reasoned legislative attempt to grapple with this serious problem.

## II. LOWER COURTS ARE CONFUSED OVER HOW TO APPLY THE OVERBREADTH DOCTRINE

VCCA § 18.2-152.3:1 is a content-neutral statute that does not generally prohibit anonymous speech on the Internet or through e-mail. The statute does not apply when a person sends e-mails using a

pseudonymous e-mail address (*e.g.*, redsoxfan@isp.com); it does not apply when a person erects and hosts an anonymous web page; it does not apply when a person anonymously posts on a blog or Internet bulletin board; it does not apply when a person uses an alias in a chat room; and it does not apply to the myriad ways that a person can speak anonymously in the tangible world.

The statute only applies when a defendant (1) infiltrates a "computer network of an electronic mail service provider or its subscribers," by (2) transmitting "unsolicited bulk electronic mail," (3) "with the intent to falsify or forge electronic mail transmission information or other routing information." The statute targets the invasion of private property—the "computer network of an electronic mail service provider or its subscribers"—and the technical falsification used to achieve that invasion.

Respondent has never contested that the VCCA is constitutional as applied to his conduct. The Virginia Supreme Court nevertheless reversed his conviction and held that the VCCA was unconstitutional on the basis of hypothetical applications of the statute not before the court. The Virginia Supreme Court did not point to any record evidence consistent with its hypothetical concerns and it pointed to no actual instances of the types of speech it worried might be impaired by the statute.

This case is the paradigmatic example of why this Court must clarify the overbreadth doctrine. The lower courts are in disarray over how to apply the overbreadth doctrine, culminating in the Virginia Supreme Court's decision to invalidate an important statute that is "surely valid 'in the vast majority of its

intended applications.'" *Hill v. Colorado*, 530 U.S. 703, 733 (2000) (citation omitted).

### A. The Overbreadth Doctrine Is "Strong Medicine" And Is Necessarily Narrow And Limited

The overbreadth doctrine is an exception to this Court's normal rules regarding facial challenges. *Virginia v. Hicks*, 539 U.S. 113, 118 (2003). Out of concern that some overly broad statutes may "chill" constitutionally protected speech, the overbreadth doctrine provides that "showing that a law punishes a 'substantial' amount of protected free speech, 'judged in relation to the statute's plainly legitimate sweep,' suffices to invalidate *all* enforcement of that law." *Id.* at 118-19 (citations omitted).

This Court has repeatedly held that such a challenge to a statute "is, manifestly, strong medicine." *Broadrick v. Oklahoma*, 413 U.S. 601, 613 (1973). For that reason, the overbreadth doctrine "has been employed by the Court sparingly and only as a last resort." *Id.*; *see also N.Y. State Club Ass'n v. City of N.Y.*, 487 U.S. 1, 11 (1988) (noting that the overbreadth doctrine is a "narrow" "exception to ordinary standing requirements"); *Hicks*, 539 U.S. at 119 (noting that "there are substantial social costs *created* by the overbreadth doctrine when it blocks application of a law to constitutionally unprotected speech, or especially to constitutionally unprotected conduct").

Therefore, in order to succeed in an overbreadth challenge, a defendant must demonstrate "*from actual fact* that a substantial number of instances exist in which the Law cannot be applied constitutionally." *N.Y. State Club Ass'n*, 487 U.S. at 14 (emphasis added). "[H]ypertechnical theories as to what a statute covers"

and "speculation about ... hypothetical situations not before the Court will not support a facial attack on a statute when it is surely valid 'in the vast majority of its intended applications.'" *Hill*, 530 U.S. at 733 (citation omitted). Also, "the mere fact that one can conceive of some impermissible applications of a statute is not sufficient to render it susceptible to an overbreadth challenge." *Members of City Council of L.A. v. Taxpayers for Vincent*, 466 U.S. 789, 800-01 (1984); *see also United States v. Williams*, 128 S. Ct. 1830, 1838 (2008).

### B. The Virginia Supreme Relied On Hypothetical Scenarios That Have No Basis in Actual Fact

To support its decision that VCCA § 18.2-152.3:1 is overbroad, the Virginia Supreme Court relied on two hypothetical scenarios: (1) the VCCA would have effectively prevented Publius from publishing the anonymous Federalist Papers had they been sent as an unsolicited bulk e-mail with forged IP address information today; and (2) the VCCA could possibly inhibit a Chinese dissident or other political dissident seeking to publicize his political views through spam. The Virginia Supreme Court divined these hypotheticals from respondent's attorneys' briefs, and from its own conjecture; no evidence in the record establishes that either scenario is realistic.

Certainly, protecting anonymous political and religious speech is vitally important, whether communicated through e-mail or any other means. However, as far as US ISPA and its members are aware, these simply are not categories of speech that are expressed by sending tens of thousands of unsolicited e-mails with forged headers designed to

evade spam filters and infiltrate private networks. US ISPA's members have vast experience in this area, and their experience confirms several realities about spam e-mail.

First, spam is overwhelmingly used to propose commercial transactions or fraudulent schemes, and to transmit malicious viruses and software. Spammers commonly seek a direct response from recipients, in the form of a sale or some other end user response, even if the spammer is shielding his identity. Spammers thus are anonymous strictly as a means to facilitate their moneymaking efforts or to evade civil or criminal prosecution for fraud, trespass, or myriad other torts and crimes. This Court's cases protecting anonymous speech, by contrast, have focused on the value a pseudonym *adds* to the quality of speech. *See, e.g., McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342-43 (1995) (noting, for example, that anonymity "provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent," and that anonymity protects "the hard-won right to vote one's conscience without fear of retaliation").

Second, those who wish to communicate religious and political messages overwhelmingly use other means, such as anonymous web pages or blogs, or even pseudonymous free e-mail accounts. US ISPA's members are not aware of spammers who are sending unsolicited bulk e-mails with falsified routing and transmission information to communicate political and religious messages in any meaningful numbers. There are no facts in the record to show that such political or religious spam even exists, and any such spam is at

most trivially small in comparison to commercial or malicious spam.[11]

Third, US ISPA is not aware of any major ISP that actually welcomes spam. To the contrary, every ISP of which US ISPA is aware not only expressly prohibits the sending of spam through its network, but takes active measures to filter and block spam messages. Spammers are sending their messages through and into private networks that affirmatively prohibit their conduct.

Finally, to unmask a spammer requires an ISP to invest substantial time, resources, and money. The notion that ISPs are interested in referring insignificant (indeed, heretofore nonexistent) volumes of political or religious speech to law enforcement—as opposed to the billions of commercial spam messages that flood their private networks every day—is farfetched. There is certainly no meaningful likelihood that any religious or political spam would ever be prosecuted under the Virginia provision in question.

It bears emphasis that the conduct for which respondent was convicted bears no connection to any of the forms of anonymous speech that are prevalent on the Internet or e-mail. Respondent was not convicted for sending e-mails using a pseudonymous e-mail

---

[11] The Virginia Supreme Court also erred by failing to recognize that Publius's ability to anonymously publish the Federalist Papers was still constrained by trespass laws. Publius could not have forced pamphlets on unwilling recipients on their own private property. The VCCA only applies to e-mails sent using private computer networks, and neither Publius nor respondent is privileged to appropriate AOL's network, or the Washington Post's advertising pages, or a privately-owned billboard, to transmit messages, regardless of content.

address; such conduct does not trigger VCCA § 18.2-152.3:1. Rather, respondent was convicted for using dozens of falsely registered domain names in order to send over 50,000 e-mails to AOL subscribers that fraudulently appeared to come from dozens of different sources in order to evade AOL's spam filters. Falsely registering domain names with affirmative misrepresentations is entirely different from the myriad ways in which people can, and do, lawfully anonymize their identities on the Internet and with e-mail.

Of course, if there are spammers who wish to transmit political or religious speech using falsified transmission information, and those spammers are unconstitutionally subject to the statute's prohibitions, they need only bring an as-applied challenge. *See Williams*, 128 S. Ct. at 1838. Such a challenge would, inevitably, produce a factual record on which to judge *actual* applications of the law to *actual* examples of protected speech. But the lesson from this Court's cases is that the overbreadth doctrine is not to be used to invalidate a statute absent actual substantial overbreadth judged in comparison to a statute's legitimate sweep.

Because actual religious or political spam is either nonexistent or trivial, the Virginia Supreme Court would have had to affirm respondent's conviction if the court had weighed any unconstitutional applications of the statute that had some basis in fact against the statute's legitimate sweep.

### C. Lower Courts Are In Disarray Over How To Apply The Overbreadth Doctrine

At a conceptual level, this Court's legal standard for evaluating a claim of overbreadth is clear. This Court has repeatedly held that a statute is facially invalid only if it prohibits a *substantial* amount of protected speech. *Williams*, 128 S. Ct. at 1838 (citing cases). Courts must judge overbreadth "not only in an absolute sense, but also relative to the statute's plainly legitimate sweep." *Id.* A challenger bears the burden to "demonstrate from the text of [the statute] and from actual fact that a substantial number of instances exist in which the Law cannot be applied constitutionally." *N.Y. State Club Ass'n*, 487 U.S. at 14.

The lower courts have struggled, however, with how to apply this standard. In particular, they have disagreed over how to determine if a statute will affect many or few instances of such speech and whether a court may simply hypothesize the extent of any unconstitutional application or instead must base any such findings on a concrete factual record. Here, the Virginia Supreme Court struck down the VCCA because it might hypothetically apply to religious sects who wish to send tens of thousands of e-mail messages to unwilling recipients with falsified transmission information, without even pausing to ask whether that theoretical overbreadth is "substantial" in any meaningful sense. It made no findings that such hypothetical speakers actually exist or in what numbers, and never considered if they would have alternative forms of communication available to them. Had this case arisen in one of a number of other jurisdictions, the statute would have upheld for the

complete absence of any evidence of an effect on actual protected noncommercial speech.

The petition identifies a number of courts, like the Virginia Supreme Court below, that have not hesitated to invent or presume facts regarding the substantiality of any overbreadth. For example, the Eighth Circuit recently invalidated a provision of a federal bankruptcy statute by hypothesizing a few potential unconstitutional applications, and then concluding that "[f]actual scenarios other than these few hypothetical situations no doubt exist." *Milavetz, Gallop & Milavetz, P.A. v. United States*, 541 F.3d 785, 794 (8th Cir. 2008); *see also State v. Casey*, 876 P.2d 138, 140-141 (Idaho 1994) (invalidating statute based on single hypothetical application). By contrast, the petition identifies other courts that apply much more rigorous mechanisms and decline to hold a statute facially invalid unless there is evidence that any overbreadth is substantial *as a matter of actual fact* in comparison to the statute's legitimate sweep.

Everything turns on that distinction. The scope and impact of the overbreadth doctrine depend entirely on how courts *apply* this Court's standard. A jurisdiction in which judges make findings about whether hypothetical applications of a statute are likely or unlikely has a very different (and far less constrained) overbreadth doctrine than a jurisdiction that requires challengers to demonstrate substantial overbreadth in actual fact. On that point the lower courts are in dire need of guidance.

Undoubtedly, some examples of protected speech may be so obvious or common that a court does not need to point to empirical evidence to invalidate a statute. No one would argue that a challenger needs

statistical studies to persuade a court that a statute prohibiting all speech in public parks is substantially overbroad. But in many (perhaps most) instances, how a statute's legitimate sweep compares to any potentially unconstitutional application will be non-obvious and fact-specific. In such instances the question of the degree to which a court may rely on its own instincts divorced from any factual record may be dispositive. As this case demonstrates, challengers should bear some burden to establish that any potential overbreadth is real, and actually substantial in comparison to the statute's legitimate sweep.

This case presents the issue squarely, as the Virginia Supreme Court's decision invalidated an important state statute targeting serious criminal conduct based on a purely hypothetical concern with overbreadth. That cannot be what this Court had in mind.

## CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

JENNIFER C. ARCHIE
*Counsel of Record*
ALEXANDER MALTAS
CATHERINE A. BELLAH
LATHAM & WATKINS LLP
555 11TH STREET, NW
SUITE 1000
WASHINGTON, DC 20004
(202) 637-2200